Notice of Allowability	Application No.	Applicant(s)	
	09/916,981	MUTTIK ET AL.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6/3/2005*.

2. ☒ The allowed claim(s) is/are *1-3,8,10-17,22 and 24-33*.

3. ☒ The drawings filed on *26 July 2001* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20050624* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Kevin Zilka on June 23, 2005.

IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) A method for detecting viruses in software, comprising:

(a) comparing subject data with a plurality of virus definitions in a first database;

(b) executing a security event if the subject data is successfully compared with at least one of the virus definitions;

(c) comparing the subject data with fingerprints of innocent data in a second database;

(d) allowing access to the subject data if the subject data is successfully compared to the fingerprints of innocent data;

(e) transmitting information to a server for analysis purposes if the subject data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data, wherein the information transmitted to the server includes a fingerprint associated with the subject data;

(f) comparing the fingerprint associated with the subject data and fingerprints associated with innocent data in a third database at the server;

(g) comparing the fingerprint associated with the subject data and fingerprints associated with virus definitions in a fourth database at the server; and

(h) transmitting the subject data to the server utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data and fingerprints associated with the innocent data in the third database and the virus definitions in the fourth database at the server;

~~wherein the information transmitted to the server includes at least one of the subject data and a fingerprint associated with the subject data;~~

wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

2. (Previously Amended) The method as recited in claim 1, wherein the security event is selected from the group consisting of cleaning the subject data, quarantining the subject data, and blocking the subject data.

3. (Previously Amended) The method as recited in claim 1, and further comprising reporting that the subject data is innocent if the subject data is successfully compared to the fingerprints of innocent data.

4.-7. (Cancelled)

8. (Previously Amended) The method as recited in claim 1, wherein the third and fourth databases are updated more frequently than the first and second databases.

9. (Cancelled)

10. (Previously Amended) The method as recited in claim 1, and further comprising analyzing the subject data transmitted to the server.

11. (Previously Amended) The method as recited in claim 1, wherein the subject data is transmitted to the server in separate parts.

12. (Original) The method as recited in claim 10, and further comprising updating at least one of the first database, the second database, the third database, and the fourth database based on the analysis.

13. (Original) The method as recited in claim 1, wherein the information is transmitted to the server via the Internet.

14. (Previously Amended) The method as recited in claim 1, wherein the first database and the second database are both components of a client computer coupled to the server via a network.

15. (Currently Amended) A computer program product for detecting viruses in software, comprising:

(a) computer code for comparing subject data with a plurality of virus definitions in a first database;

(b) computer code for executing a security event if the subject data is successfully compared with at least one of the virus definitions;

(c) computer code for comparing the subject data with fingerprints of innocent data in a second database;

(d) computer code for allowing access to the subject data if the subject data is successfully compared to the fingerprints of innocent data;

(e) computer code for transmitting information to a server for analysis purposes if the subject data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data, wherein the information transmitted to the server includes a fingerprint associated with the subject data;

(f) computer code for comparing the fingerprint associated with the subject data and fingerprints associated with innocent data in a third database at the server;

(g) computer code for comparing the fingerprint associated with the subject data and fingerprints associated with virus definitions in a fourth database at the server; and

(h) computer code for transmitting the subject data to the server utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data and fingerprints associated with the innocent data in the third database and the virus definitions in the fourth database at the server;

~~wherein the information transmitted to the server includes at least one of the subject data and a fingerprint associated with the subject data;~~

wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

16. (Previously Amended) The computer program product as recited in claim 15, wherein the security event is selected from the group consisting of cleaning the subject data, quarantining the subject data, and blocking the subject data.

17. (Previously Amended) The computer program product as recited in claim 15, and further comprising computer code for reporting that the subject data is innocent if the subject data is successfully compared to the fingerprints of innocent data.

18.-21. (Cancelled)

22. (Previously Amended) The computer program product as recited in claim 15, wherein the third and fourth databases are updated more frequently than the first and second databases.

23. (Cancelled)

24. (Previously Amended) The computer program product as recited in claim 15, and further comprising computer code for analyzing the subject data transmitted to the server.

25. (Previously Amended) The computer program product as recited in claim 24, wherein the subject data is transmitted to the server in separate parts.

26. (Original) The computer program product as recited in claim 24, and further comprising computer code for updating at least one of the first database, the second database, the third database, and the fourth database based on the analysis.

27. (Original) The computer program product as recited in claim 15, wherein the information is transmitted to the server via the Internet.

28. (Previously Amended) The computer program product as recited in claim 15, wherein the first database and the second database are both components of a client computer coupled to the server via a network.

29. (Currently Amended) A system for detecting viruses in software, comprising:

(a) logic for comparing subject data with a plurality of virus definitions in a first database;

(b) logic for executing a security event if the subject data is successfully compared with at least one of the virus definitions;

(c) logic for comparing the subject data with fingerprints of innocent data in a second database;

(d) logic for allowing access to the subject data if the subject data is successfully compared to the fingerprints of innocent data;

(e) logic for transmitting information to a server for analysis purposes if the subject data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data, wherein the transmitted information includes a fingerprint associated with the subject data;

(f) logic for comparing the fingerprint associated with the subject data and fingerprints associated with innocent data in a third database;

(g) logic for comparing the fingerprint associated with the subject data and fingerprints associated with virus definitions in a fourth database; and

(h) logic for transmitting the subject data to the server utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data and fingerprints associated with the innocent data in the third database and the virus definitions in the fourth database;

~~wherein the transmitted information includes at least one of the subject data and a fingerprint associated with the subject data;~~

wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

30. (Currently Amended) A method for detecting viruses in software, comprising:

(a) comparing subject data with a plurality of virus definitions in a first database;

(b) executing a security event if the subject data is successfully compared with at least one of the virus definitions;

(c) comparing the subject data with fingerprints of innocent data in a second database;

(d) reporting that the subject data is innocent if the subject data is successfully compared to the fingerprints of innocent data; and

(e) transmitting a fingerprint of the subject data over a network to a server for analysis purposes if the subject data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data;

(f) comparing [a]the fingerprint associated with the subject data and fingerprints associated with innocent data in a third database;

(g) comparing the fingerprint associated with the subject data and fingerprints associated with virus definitions in a fourth database; and

(h) transmitting the subject data to the server utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data and fingerprints associated with the innocent data in the third database and the virus definitions in the fourth database;

wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

31. (Currently Amended) A method for detecting viruses in software, comprising:

(a) receiving a fingerprint associated with subject data from a client computer for analysis purposes upon the subject data being unsuccessfully compared to virus definitions and fingerprints of innocent data stored on the client computer;

(b) comparing the fingerprint associated with the subject data and ~~the~~ fingerprints associated with innocent data at a server;

(c) comparing the fingerprint associated with the subject data and fingerprints associated with virus definitions at the server;

(d) requesting the subject data from the client computer utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data, and the fingerprints associated with the innocent data and the virus definitions at the server;

(e) receiving the subject data transmitted from the client computer in response to the request;

(f) analyzing the subject data transmitted from the client computer; and

(g) updating at least one of the virus definitions and the fingerprints of innocent data based on the analysis;

wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

32. (Previously Amended) A method for detecting viruses in software, comprising:

(a) receiving a fingerprint associated with subject data from a client computer for analysis purposes upon the subject data being unsuccessfully compared to virus definitions stored on the client computer;

(b) comparing the fingerprint associated with the subject data and fingerprints associated with virus definitions at a server;

(c) requesting the subject data from the client computer utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data, and the fingerprints associated with the virus definitions at the server;

(d) receiving the subject data transmitted from the client computer in response to the request;

(e) analyzing the subject data transmitted from the client computer; and

(f) updating the virus definitions based on the analysis;

wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

33. (Previously Amended) A security method, comprising:

(a) receiving a fingerprint associated with subject data from a client computer for analysis purposes upon the subject data being unsuccessfully compared to fingerprints associated with innocent data stored on the client computer;

(b) comparing the fingerprint associated with the subject data, and fingerprints associated with innocent data at a server;

(c) requesting the subject data from the client computer utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data, and the fingerprints associated with the innocent data at the server;

(d) receiving the subject data transmitted from the client computer in response to the request;

(e) analyzing the subject data transmitted from the client computer; and

(f) updating the fingerprints associated with the innocent data based on the analysis;

wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance:

Hypponen et al. (U.S. Patent 6,577,920) discloses a macro virus detection system that utilizes three databases, the first for virus definitions, the second for commercially available macros, and the third for local macros. This system first checks to see if the detected macro is in the first database (if it contains a virus), and then proceeds to check the second and third databases to determine if the macro is an innocent macro. If the macro is not detected in any of these databases, access to the file is halted, and a report is sent to a network manager and a remote server, as shown in the action dated 4/26/2005.

Vibert (Vibert, R., "A Day in the Life of an Anti-Virus Lab", 6/17/2000, pp. 1-5) discloses that the data is sent to a remote server when the local computer cannot discern whether the file contains a virus or not. Once at this remote server, the data is checked to determine if it is definitely innocent by using a database of innocent fingerprints to compare the data to. If it is not found to be innocent, then the server will run various anti-virus programs to determine if the data contains a virus. If the anti-virus programs fail to detect a virus in the file, then the data is inspected by virus analysts (or automated heuristic programs) to determine, with precision, if the file contains a virus or is innocent, as shown in the action dated 4/26/2005.

What is missing from the prior art is transmitting a fingerprint of the data to the server to be analyzed and, only when the server determines that it needs the full data,

will the client transmit the full data to the server within the system of Hypponen et al. as modified by Vibert.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER